

Accessing quantum secrets via local operations and classical communication

Vlad Gheorghiu^{1,2,*} and Barry C. Sanders¹

¹*Institute for Quantum Science and Technology, University of Calgary, Calgary, AB, T2N 1N4, Canada*

²*Department of Mathematics and Statistics, University of Calgary, Calgary, AB, T2N 1N4, Canada*

(Dated: Version of May 3, 2013)

Quantum secret-sharing and quantum error-correction schemes rely on multipartite decoding protocols, yet the non-local operations involved are challenging and sometimes infeasible. Here we construct a quantum secret-sharing protocol with a reduced number of quantum communication channels between the players. Our scheme is based on embedding a classical linear code into a quantum error-correcting code. Our work paves the way towards the more general problem of simplifying the decoding of quantum error-correcting codes.

PACS numbers: 03.67.Dd, 03.67.Pp, 03.67.Mn

Secret sharing is a cryptographic protocol in which a dealer distributes a shared secret among a set of players, so that only certain authorized subsets can collaboratively recover the secret. The protocol, first introduced by Shamir [1] and Blakley [2], is important in any area that requires sharing of highly sensitive information, such as bank accounts, missile launch sequences etc.

The quantum counterpart is a scheme in which the dealer distributes either a classical secret [3] (string of bits) or a quantum secret (quantum state) [4] to the set of players via quantum channels [5, 6]. Quantum secret-sharing is useful for distributing shared quantum keys, non-counterfeitable “quantum money” [7], distributed quantum computing [8], secure quantum memory and multipartite quantum communication [9]. For the quantum secret-sharing protocol to be feasible, the dealer is assumed to be “powerful” – she can prepare arbitrary quantum states and reliably distribute them to the players. The players have full access to universal quantum computers and can communicate among themselves via quantum channels so that only certain authorized subsets can recover (decode) the secret. The decoding operation is harder to implement than in the classical case, as it requires quantum communication which is expensive.

Reducing the amount of quantum communication required for the decoding can improve the efficiency of distributed cryptographic protocols in which a subset of the players have restricted communication capabilities. Consider for example a quantum secret-sharing scheme with players divided into two subsets, one of which is computationally powerful (each player has access to universal quantum computation and all players can use quantum communication), whereas the other one is computationally weak (each player has access to local universal quantum computers but the players can use only classical communication between them). One such instance is a secret-sharing scheme between the Earth (the computationally powerful subset) and e.g. the International Space Station (the computationally weak subset).

Reducing the amount of quantum communication (i.e. reducing the number of non-local operations involved) also helps simplifying the decoding of quantum error-correcting codes [10, 11], which are of crucial importance for the construction of a real-world fault-tolerant quantum computer.

In this article we solve the following problem. For a large class of quantum secret-sharing schemes constructed from classical linear error-correcting codes [12], we show that their decoding can be simplified by replacing some of the quantum channels among the players by classical ones. Inspired by the Calderbank-Shore-Steane (CSS) construction [13] we embed a classical linear error-correcting code into a quantum code, then show that this embedding induces a quantum secret-sharing scheme in which all players have to collaborate to recover the secret. In this protocol some of the players are only required to perform local measurements and share their measurement results via classical channels.

We begin by considering an $[n, k, d]_q$ classical error-correcting code over \mathbb{F}_q , the Galois field with $q = p^m$ elements, where p is prime and m is a positive integer. The parameter k denotes the number of encoded *dits* (generalization of a bit that allows holding more than 2 states), n is the number of carriers and d is the distance of the code. We can represent such a code compactly using a $k \times n$ *generator matrix* G with elements in \mathbb{F}_q . Each codeword (n -tuple in \mathbb{F}_q^n [14]) can then be written as

$$\mathbf{x} \cdot G = \sum_{ij} x_i G_{ij}, \quad (1)$$

where \mathbf{x} is a k -tuple in \mathbb{F}_q^k , for a total number of codewords equal to q^k , where the addition and multiplication in (1) are over the finite field \mathbb{F}_q . One can regard G as a linear mapping from the ‘input’ space \mathbb{F}_q^k to the ‘output’ (or encoded) subspace of \mathbb{F}_q^n , see the top of our diagram (mapping 1) in Fig. 1.

We use the elements $\mathbf{x} \in \mathbb{F}_q^k$ to label the basis vectors of $\mathcal{H}^{\otimes k}$, the Hilbert space of k qudits, and denote the collection of the orthonormal basis vectors by $\{|\mathbf{x}\rangle\}_{\mathbf{x} \in \mathbb{F}_q^k}$, see the mapping 4 in Fig. 1. Similarly we embed the elements $\mathbf{x} \cdot G \in \mathbb{F}_q^n$ into a subspace of the $\mathcal{H}^{\otimes n}$ spanned

* vgheorgh@ucalgary.ca

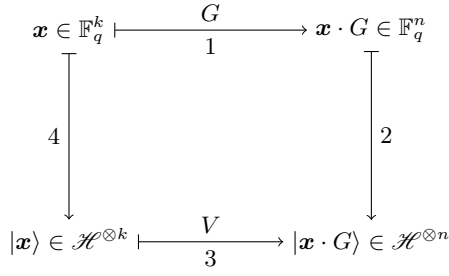


FIG. 1. A schematic for various embeddings used throughout the article.

by the collection of orthonormal vectors $\{|\mathbf{x} \cdot G\rangle\}_{\mathbf{x} \in \mathbb{F}_q^k}$, as depicted by mapping 2 in Fig. 1. Note that $\mathcal{H}^{\otimes k}$ is isomorphic with $\text{Span}\{|\mathbf{x} \cdot G\rangle\}_{\mathbf{x} \in \mathbb{F}_q^k}$ through an encoding isometry V , see the bottom of our diagram (mapping 3) in Fig. 1. In particular, the isometry V can be explicitly constructed from the generating matrix G using a simple quantum circuit that consists of Control-NOT gates; see § 10.5.8 of [13].

We have all the ingredients to construct a quantum secret-sharing scheme as follows. A dealer holds a k -qudit quantum secret

$$|\psi\rangle = \sum_{\mathbf{x} \in \mathbb{F}_q^k} c(\mathbf{x})|\mathbf{x}\rangle, \quad (2)$$

with $c(\mathbf{x})$ normalized complex coefficients. The secret is then distributed to a set of n players using the isometric encoding V , so the state shared by the players is

$$|\Psi\rangle = \sum_{\mathbf{x} \in \mathbb{F}_q^k} c(\mathbf{x})|\mathbf{x} \cdot G\rangle. \quad (3)$$

We next design a decoding protocol in which all n players have to collaborate; however, just a proper subset A of the entire set of players P is required to use local operations and classical communication (LOCC) with the complementary subset B . The latter subset can then fully recover the quantum secret. Our scheme is depicted in Fig. 2. Our secret-sharing scheme is imperfect (or ‘ramp’), i.e. there exist subsets of players that may extract partial information about the secret. However, we can transform it to a perfect (or ‘threshold’) quantum secret-sharing scheme via ‘twirling’ and allowing the dealer to share extra classical communication channels with the players [15, 16].

Definition. A subset A of the entire set of players P is LOCC-assisting for its complement B whenever there exists an LOCC scheme that A can perform, followed by sending the measurement results to B , so that B can fully recover the quantum secret.

Inspired by the CSS construction, we employ the concept of embedding a classical code into a quantum code,

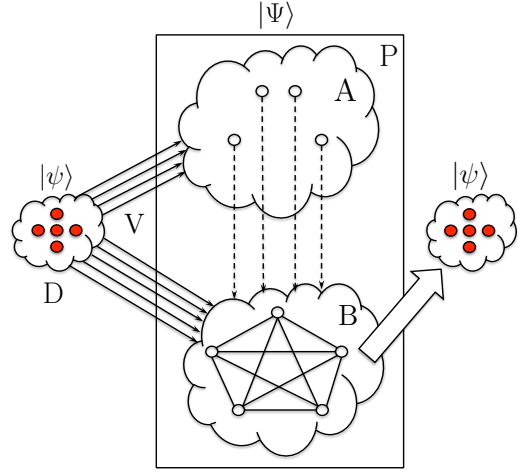


FIG. 2. LOCC-recoverable quantum secret-sharing. The dealer D encodes k qudits (filled in circles) in state $|\psi\rangle$ via the isometry V to realize the state $|\Psi\rangle$, then transmits it to the players P (with each player denoted by an empty circle) via quantum channels (solid lines indicate single-qudit channels). The players in A perform local measurements and each one communicates via classical channels (dashed lines) with all players in B , who are all connected via quantum channels. Finally the players in B perform a global quantum operation to recover $|\psi\rangle$.

but use the technique to construct a novel way of decoding quantum secret-sharing schemes. The most important outcome of our scheme is a drastic reduction of the number of inter-player quantum communication channels required for the decoding. Our main result is summarized below.

Theorem 1. Let $[n, k, d]_q$ be a classical error-correcting code with generator matrix G , and let $|\Psi\rangle$ be a k -qudit quantum secret distributed to a set of n players using the isometric encoding

$$|\mathbf{x}\rangle \xrightarrow{V} |\mathbf{x} \cdot G\rangle. \quad (4)$$

Let A be a subset of the carrier qudits, and let B denote its complement. Let G_B be the matrix obtained by removing the columns that correspond to the players in B from G . Then the subset A is LOCC-assisting for its complement B if and only if

$$\text{rank}(G_B) = k. \quad (5)$$

Proof. Consider that each player in A performs a local measurement in the Fourier basis $\{|\bar{x}\rangle = F|x\rangle\}_{x \in \mathbb{F}_q}$, where F is the generalized Fourier matrix defined as

$$F := \frac{1}{\sqrt{q}} \sum_{x, z \in \mathbb{F}_q} \omega^{\text{tr}(xz)} |z\rangle \langle x|, \quad \omega := \exp(2\pi i/p), \quad (6)$$

where $\text{tr}(x)$ denotes the ‘trace’ [17, 18] of an element $x \in \mathbb{F}_{q=p^m}$,

$$\text{tr} : \mathbb{F}_q \longrightarrow \mathbb{F}_p, \quad x \xrightarrow{\text{tr}} \sum_{i=0}^{m-1} x^{p^i} \in \mathbb{F}_p. \quad (7)$$

We denote by $a_k \in \mathbb{F}_q$ the label of the measurement result of the k -th player. For compactness we collect all measurement results that the players in A perform into a vector $\mathbf{a} \in \mathbb{F}_q^{|A|}$, where $|A|$ represents the number of players in A . Let

$$|\Psi\rangle_{B,\mathbf{a}} := \frac{\text{Tr}_A[(|\mathbf{a}\rangle\langle\mathbf{a}| \otimes I_B)|\Psi\rangle]}{\|\text{Tr}_A[(|\mathbf{a}\rangle\langle\mathbf{a}| \otimes I_B)|\Psi\rangle]\|} \quad (8)$$

be the normalized resultant state of the remaining B players, given that the results of the measurements by A are \mathbf{a} . From (6) all measurement results have the same probability, independent of the secret $|\psi\rangle$ in (2),

$$p(\mathbf{a}) = \|\text{Tr}_A[(|\mathbf{a}\rangle\langle\mathbf{a}| \otimes I_B)|\Psi\rangle]\|^2 = \frac{1}{q^{|A|}}. \quad (9)$$

The resultant state on B , given the measurement result \mathbf{a} , is

$$|\Psi\rangle_{B,\mathbf{a}} = \sum_{\mathbf{x} \in \mathbb{F}_q^k} c(\mathbf{x}) \omega^{-\text{tr}(\mathbf{x} \cdot G_A \cdot \mathbf{a}^T)} |\mathbf{x} \cdot G_B\rangle. \quad (10)$$

Note that $\text{rank}(G_B) \leq k$, as G_B is obtained from the rank- k generator matrix G by removing columns from the latter.

If $\text{rank}(G_B) < k$, the number of mutually orthogonal states in (10) is less than the dimension q^k of the quantum secret $|\psi\rangle$ in (2), or, equivalently, $\dim(\text{span}(\{|\mathbf{x} \cdot G_B\rangle\}_{\mathbf{x} \in \mathbb{F}_q^k})) < \dim(\text{span}(\{|\mathbf{x}\rangle\}_{\mathbf{x} \in \mathbb{F}_q^k}))$. In this case it is impossible to map the state $|\Psi\rangle_{B,\mathbf{a}}$ in (10) back to $|\psi\rangle$ by an isometry that does not depend on the coefficients $c(\mathbf{x})$; there is not enough “space” to “fit” the secret $|\psi\rangle$ in the state $|\Psi\rangle_{B,\mathbf{a}}$ and information is irreversibly lost [19, 20].

On the other hand the vectors $\{|\mathbf{x} \cdot G_B\rangle\}_{\mathbf{x} \in \mathbb{F}_q^k}$ are mutually orthogonal if and only if $\text{rank}(G_B) = k$. In this latter case, the state $|\Psi\rangle_{B,\mathbf{a}}$ can be mapped back to the original secret $|\psi\rangle$ via a *decoding isometry* (that depends on the measurement results \mathbf{a}) defined via

$$|\mathbf{x} \cdot G_B\rangle \mapsto \omega^{\text{tr}(\mathbf{x} \cdot G_A \cdot \mathbf{a}^T)} |\mathbf{x}\rangle. \quad (11)$$

□

Our next result shows how to construct the above decoding isometry explicitly.

Theorem 2. *Let A be an LOCC-assisting subset for its complement B . Then the decoding isometry for B is a product of a local unitary operation, which depends only on the measurement results \mathbf{a} , and an isometry that depends only on the subset B . A corresponding decoding quantum circuit can be constructed explicitly.*

Proof. For some $\mathbf{z} \in \mathbb{F}_q^{n-|A|}$ consider the action of $Z^{\mathbf{z}} := Z^{z_1} \otimes \dots \otimes Z^{z_{n-|A|}}$ on $|\Psi\rangle_{B,\mathbf{a}}$ in (10), where Z^z is the generalized single-qudit Weyl-Heisenberg operator [17, 18] defined as

$$Z^z := \sum_{x \in \mathbb{F}_q} \omega^{\text{tr}(zx)} |x\rangle\langle x|, \text{ for } z \in \mathbb{F}_q. \quad (12)$$

The resultant state is

$$\begin{aligned} Z^{\mathbf{z}} |\Psi\rangle_{B,\mathbf{a}} &= \sum_{\mathbf{x} \in \mathbb{F}_q^k} c(\mathbf{x}) \omega^{-\text{tr}(\mathbf{x} \cdot G_A \cdot \mathbf{a}^T)} Z^{\mathbf{z}} |\mathbf{x} \cdot G_B\rangle \\ &= \sum_{\mathbf{x} \in \mathbb{F}_q^k} c(\mathbf{x}) \omega^{-\text{tr}(\mathbf{x} \cdot G_A \cdot \mathbf{a}^T)} \omega^{\text{tr}(\mathbf{x} \cdot G_B \cdot \mathbf{z}^T)} |\mathbf{x} \cdot G_B\rangle \\ &= \sum_{\mathbf{x} \in \mathbb{F}_q^k} c(\mathbf{x}) \omega^{\text{tr}[\mathbf{x} \cdot (G_B \cdot \mathbf{z}^T - G_A \cdot \mathbf{a}^T)]} |\mathbf{x} \cdot G_B\rangle. \end{aligned} \quad (13)$$

We now claim that there always exists a $\mathbf{z} \in \mathbb{F}_q^{n-|A|}$ such that

$$G_B \cdot \mathbf{z}^T = G_A \cdot \mathbf{a}^T. \quad (14)$$

As A is LOCC-assisting for B , Theorem 1 implies that $\text{rank}(G_B) = k$. This fact implies that (14) admits at least one solution \mathbf{z} which can be found by elementary linear algebra methods over finite fields. Therefore, for such a solution \mathbf{z} , the operator $Z^{\mathbf{z}}$ eliminates all phases in (10)

$$Z^{\mathbf{z}} |\Psi\rangle_{B,\mathbf{a}} = \sum_{\mathbf{x} \in \mathbb{F}_q^k} c(\mathbf{x}) |\mathbf{x} \cdot G_B\rangle, \quad (15)$$

which implies at once that the resultant state (15) can be mapped back to the original secret (2) by an isometry V_B defined by

$$|\mathbf{x} \cdot G_B\rangle \xrightarrow{V_B} |\mathbf{x}\rangle. \quad (16)$$

The overall recovery procedure can be written as $V_B Z^{\mathbf{z}}$, where V_B is independent of the measurement results and depends only on the subset B , and $Z^{\mathbf{z}}$ is a local unitary correction that depends only on the measurement results \mathbf{a} . The isometry V_B is the adjoint of the quantum circuit that maps $|\mathbf{x}\rangle$ to $|\mathbf{x} \cdot G_B\rangle$, and can be constructed explicitly, similarly to the construction of the encoding isometry V . □

As our goal is to reduce the number of quantum communication channels among the players, we aspire to construct schemes in which the LOCC-assisting subsets A are as large as possible. The restriction $|B| \geq k$ must be satisfied, as otherwise information is lost and thus there is no way for B to recover the quantum secret faithfully [19]. We now show that there exist ‘optimal’ schemes for which $|B| = k$, which requires the following Lemma.

Lemma 3. *Every subset B of size $|B| > n - d$, where d is the distance of the underlying classical $[n, k, d]_q$ code, can fully recover the secret $|\psi\rangle$ by LOCC assistance from its complement A .*

Proof. This follows at once as the distance d of the classical code is

$$d = 1 + \max_r [\text{rank}(G_B) = k, \forall B \text{ with } |B| = n - r], \quad (17)$$

which is to say that one can arbitrarily remove at most $d - 1$ columns from the generator matrix G without changing the rank of the resultant G_B . Therefore, the maximum r in (17) is $d - 1$, which implies that the minimum size of B has to be at least $n - (d - 1) = n - d + 1$. □

Lemma 3 implies at once that efficient (in terms of quantum communication) LOCC-recoverable secret-sharing schemes are obtained from classical $[n, k, d]_q$ codes that maximize the distance for fixed n and k . Such an example is constituted by the class of maximum distance separable (MDS) codes that achieve equality in the classical Singleton bound [13],

$$n - k = d - 1. \quad (18)$$

Theorem 4. *An MDS classical code $[n, k, n - k + 1]_q$ induces a quantum secret-sharing scheme in which every subset B of size k or more can recover the quantum secret by LOCC assistance from its complement A . Furthermore, if $|B| = k$, the scheme is optimal in terms of the number of quantum communication channels required among the players.*

Proof. The proof follows immediately from Lemma 3. \square

We illustrate our formalism by a concrete example (simple enough to be worked out by hand).

Example 1. *Consider a classical repetition code $[n = 3, k = 1, d = 3]_2$ with generator matrix $G = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$ and note that this is an MDS code. The corresponding classical codewords 000 and 111 are embedded into two quantum states, $|000\rangle$ and $|111\rangle$, respectively. A secret $|\psi\rangle = c(0)|0\rangle + c(1)|1\rangle$ is distributed to three players as $|\Psi\rangle = c(0)|000\rangle + c(1)|111\rangle$. Theorem 4 implies that any subset B of size $|B| \geq 1$ can recover the secret by requiring the players in A to perform measurements in the $\{|+\rangle, |-\rangle\}$ basis and then send the measurement results back to B .*

Without loss of generality assume that the players 1 and 2 perform measurements, with measurement results $a_1 \in \mathbb{F}_2$ and $a_2 \in \mathbb{F}_2$, respectively. The resultant state on the third player is

$$|\Psi\rangle_{\{3\}, \mathbf{a}} = c(0)|0\rangle + (-1)^{a_1 \oplus a_2} c(1)|1\rangle, \quad (19)$$

where \oplus denotes addition mod 2. Whenever a_1 and a_2 have the same parity, the third player does not have to do anything. When a_1 and a_2 are different, then the third

player has to apply a Z operator to remove the phase in (19). The combined effect can be achieved by player 3 applying the operator $Z^{a_1 \oplus a_2}$.

Applying directly our formalism, we have $A = \{1, 2\}$, $B = \{3\}$, $G_A = \begin{pmatrix} 1 & 1 \end{pmatrix}$ and $G_B = \begin{pmatrix} 1 \end{pmatrix}$. Using (10) we can write the resultant state $|\Psi\rangle_{\{3\}, \mathbf{a}}$ after the measurement performed by the subset A in exactly the same form as (19). The operator Z^z the player $B = \{3\}$ has to apply can be found using (14), which yields

$$z = \begin{pmatrix} 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} a_1 & a_2 \end{pmatrix}^T = a_1 \oplus a_2, \quad (20)$$

as shown below (19). This example was first described in the seminal paper of Hillery et al [3].

The above scheme can be generalized at once to $n > 3$ generalized GHZ states over larger alphabets by using a classical MDS repetition code $[n, 1, n]_q$ over \mathbb{F}_q with generator matrix $G = \begin{pmatrix} 1 & 1 & \dots & 1 \end{pmatrix}$. The $\{|\pm\rangle\}$ measurement basis is now replaced by the Fourier basis $\{|\bar{x}\rangle\}_{x \in \mathbb{F}_q}$. For a faithful decoding, the n -th player must apply the operator Z^z , with $z = \bigoplus_{i=1}^{n-1} a_i$, where the sum is taken over the elements of \mathbb{F}_q .

In summary, we have developed a novel qudit quantum secret-sharing protocol in which we reduce the quantum communication overhead among the players by enabling some quantum channels to be replaced by classical ones. Our scheme is based on embedding a classical linear code into a quantum code, then using the latter for the actual construction of the protocol. The size of the LOCC-assisting subsets is determined entirely by the error-correcting properties of the classical code.

As quantum secret-sharing schemes are a form of quantum error-correction, our results represent a first step towards attacking the challenging problem of minimizing the amount of quantum communication needed for decoding the latter.

We acknowledge financial support from the Natural Sciences and Engineering Research Council (NSERC) of Canada and from the Pacific Institute for the Mathematical Sciences (PIMS). B.C.S. acknowledges additional support from CIFAR.

-
- [1] A. Shamir, Commun. ACM **22**, 612 (1979).
 - [2] G. Blakley, Proc. AFIPS **48**, 313 (1979).
 - [3] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).
 - [4] R. Cleve, D. Gottesman, and H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999).
 - [5] D. Markham and B. C. Sanders, Phys. Rev. A **78**, 042309 (2008).
 - [6] A. Keet, B. Fortescue, D. Markham, and B. C. Sanders, Phys. Rev. A **82**, 062315 (2010).
 - [7] S. Wiesner, Sigact News **15**, 78 (1983).
 - [8] M. Ben-Or, C. Crepeau, D. Gottesman, A. Hassidim, and A. Smith, in *Foundations of Computer Science, 2006. FOCS '06. 47th Annual IEEE Symposium on* (2006) pp. 249–260.
 - [9] T. Eggeling and R. F. Werner, Phys. Rev. Lett. **89**, 097905 (2002).
 - [10] P. W. Shor, Phys. Rev. A **52**, R2493 (1995).
 - [11] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996).
 - [12] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes* (North-Holland Mathematical Library, Amsterdam, 1977).
 - [13] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 5th ed. (Cambridge University Press, Cambridge, 2000).

- [14] Throughout the paper we represent tuples as row vectors, and use the transpose symbol T to denote a column vector.
- [15] B. Fortescue and G. Gour, IEEE Trans. Inf. Theor. **58**, 6659 (2012).
- [16] V. Gheorghiu, Phys. Rev. A **85**, 052309 (2012).
- [17] D. Gottesman, “Stabilizer codes and quantum error correction,” E-print arXiv:quant-ph/9705052.
- [18] M. Grassl, M. Rötteler, and T. Beth, International Journal of Foundations of Computer Science **14**, 757 (2003).
- [19] D. Gottesman, Phys. Rev. A **61**, 042311 (2000).
- [20] R. B. Griffiths, Phys. Rev. A **76**, 062320 (2007).